DETAILED ACTION

Response to Arguments

1. In communications filed on 7/23/2008, applicant has amended claims 46, 64, 65, and 67. The following claims 46-70 are presented for examination.

1.1 Applicant's arguments, pages 7-10 filed on 7/23/2008, with respect to the art rejection of claims 46-70 have been fully considered, but they are not persuasive. Applicant argues that in Feiken the identification unit processes data packet headers in sequence. Examiner respectfully disagrees as Feiken discloses each processing unit may have its own buffer (see column 4, lines 21-25. In addition, the control means can assign data packets to more than one channel in parallel (see column 4, lines 25-48). Applicant's IDS also discloses parallel classification of data packets. Upon further consideration, a new ground of rejection is made in view of Feiken and Ellis. The rejection of the dependent claims not challenged by applicant can still be applied in this office action.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 10/6/2008 was filed after the mailing date of the Non-Final Rejection on 1/23/2008. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 46-62 and **64-66** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,484,257 to **Ellis**.

As per claim 46, **Feiken et al** discloses a device comprising: an identification unit (classification module) in the device that determines security association information associated with a data flow between a source and destination (see column 3, line 65 through column 4, line 5); a plurality of processing units coupled to the identification unit that meets the recitation of a plurality of processing engines coupled to the classification module (see column 3, lines 59-65), each of the plurality of security processing engines configured to receive at least a portion of the security association information associated with a data packet in the plurality of data packets along with the corresponding data packet (see column 4, lines 7-25), wherein at least two of the plurality of security processing engines receive security association information for different

packets (see column 4, lines 25-41); wherein the classification module (identification unit) is configured to provide at least a portion of the security association information associated with the data packets to the plurality of security processing engines (see column 3, line 65 through column 4, line 8); wherein the plurality of security processing engines are configured to process a plurality of the data packets in parallel (see column 4, lines 25-41). Although not specifically stated that the classification module is configured to determine the security association information associated for the plurality of data packets simultaneously, **Feiken et al** discloses each processing unit may have its own buffer (see column 4, lines 21-25) and since different channels can be used to assign data packets, it is clear to one of ordinary skill in the art that the control means could assign data packets to more than one channel in parallel (see column 4, lines 25-48). **Ellis** in an analogous art further discloses IPSec protocol for implementing security association information wherein the device is configured to determine the security association information associated for the plurality of data packets simultaneously (see **Ellis**, column 8, line 62 through column 9, line 12 and fig. 5A). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of **Feiken et al** to determine the security association information associated for the plurality of data packets simultaneously as suggested by **Ellis** so as to achieve further increase in speed.

As per claims 47-48, **Feiken et al** discloses the limitation of further comprising a memory in the identification unit for storing security association information of a data packet, information belonging to the channel, key and status information (see column 4, lines 1-13 and column 5, lines 17-21) that meets the recitation of a database including security association

information wherein the database is local to the classification module, and wherein the database includes one or more entries wherein each entry defines information associated with one security association.

As per claim 49, **Feiken et al** discloses the limitation of wherein the database is located on the same chip as the classification module, for example (see column 5, lines 17-21).

As per claim 54, **Feiken et al** discloses using security association information in the data packets to perform cryptographic operation that meets the recitation of wherein the security association information includes protocol mode information, (see column 5, lines 37-60 and column 6, lines 9-13).

As per claim 55, **Feiken et al** discloses wherein the database (the organized information as disclosed in claims 47-48) is stored in memory.

As per claim 56, **Feiken et al** discloses wherein the memory is contact addressable memory (CAM) (see column 5, lines 17-21).

As per claim 57, **Feiken et al** discloses wherein the memory is random-access memory (see column 6, lines 49-52).

As per claim 60, **Feiken et al** discloses wherein the device is a network communication device (see column 3, lines 20-22).

As per claim 64, **Feiken et al** discloses a method for classifying data packets during security processing in a server (device) comprising: receiving in the device at least a portion of a header for each data packet in a plurality of data packets associated with a data flow between a source and destination (see column 3, line 65 through column 4, line 5); **Feiken et al** discloses each data packet in a plurality of data packets associated with a data flow between a source and destination (see column 1, lines 13-33); **Feiken et al** discloses determining security association information associated with each data packet in the plurality of data packets in the data flow, for example (see column 3, line 65 through column 4, line 5); **Feiken et al** discloses receiving at least a portion of the security association information associated with a data packet in the plurality of data packets along the with the corresponding data packet at each security processing engine in a plurality of security processing engines in the device (see column 4, lines 7-25), wherein at least two of the plurality of security processing engines receive security association information for different packets in the data flow (see column 4, lines 25-41) and processing the plurality of data packets in the data flow in parallel (see column 4, lines 25-41). Although not specifically stated that the classification module is configured to determine the security association information associated for the plurality of data packets simultaneously, **Feiken et al** discloses each processing unit may have its own buffer (see column 4, lines 21-25) and since different channels can be used to assign data packets, it is clear to one of ordinary skill in the art that the control means could assign data packets to more than one channel in parallel (see column

4, lines 25-48). **Ellis** in an analogous art further discloses IPSec protocol for implementing security association information wherein the device is configured to determine the security association information associated for the plurality of data packets simultaneously (see **Ellis**, column 8, line 62 through column 9, line 12 and fig. 5A). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of **Feiken et al** to determine the security association information associated for the plurality of data packets simultaneously as suggested by **Ellis** so as to achieve further increase in speed.

As per claim 65, **Feiken et al** discloses the limitation of wherein the step of determining security association information comprises accessing a database to determine security association information (see column 6, lines 9-13).

As per claim 66, **Feiken et al** discloses using one or more selectors to identify a security association information entry in the database (see column 7, lines 18-25).

As per claim 50, **Feiken et al** substantially discloses the claimed device of claim 46. **Feiken et al** is silent about the particular information included in the header. **Ellis** in an analogous art further discloses IPSec protocol for implementing security association information which meets the recitation of wherein the security association information includes a sequence number an anti-replay window and a lifetime of the security association, one of ordinary skill in the art would recognize these properties as part of IPSec security protocol information (see **Ellis**, column 3, lines 15-64). Therefore, it would have been obvious to one of ordinary skill in the art

at the time the invention was made to implement the device of **Feiken et al** to determine IPSec security protocol information as well known practice in the art to provide secure communications in processing data packets as suggested by **Ellis** (see column 3, lines 15-17).

As per claim 51, the references as combined above disclose the limitation of wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys, for example (see **Ellis**, column 3, lines 15-64). This claim is also rejected on the same rationale as the rejection of claim 50 above.

As per claims 52-53, the references as combined above disclose the limitation of wherein the security association information further includes an (ESP) authentication algorithm identifier and one or more ESP authentication keys and an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys, for example (see **Ellis**, column 3, lines 15-64). This claim is also rejected on the same rationale as the rejection of claim 50 above.

As per claims 58-59 and 61, **Feiken et al** substantially discloses the claimed device of claim 46. It is obvious to one of ordinary skill in the art that the invention as combined above can be implemented in different communication device such as router, firewall, or gateway device to provide routing table computations and network management (see **Ellis**, column 8, lines 33-36 and column 9, lines 29-43 and fig. 7).

As per claim 62, **Feiken et al** substantially discloses the claimed device of claim 46 and **Ellis** further discloses wherein the device is a server (see **Ellis**, column 8, lines 58-66). This claim is also rejected on the same rationale as the rejection of claim 50 above.

4. **Claims 67-70** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,484,257 to **Ellis** as applied to claims 64-66 and further in view of US Patent 6,760,444 to **Leung**.

As per claim 67, **Feiken et al** substantially discloses the claimed method of claim 66. **Feiken et al** is silent about the particular selectors included in the header. **Leung** in an analogous art discloses wherein the step of determining security association information comprises accessing a database to determine security association information (see column 6, lines 13-28) and further comprises using one or more selectors to identify a security association information entry in the database wherein the one or more selectors include at least one of a destination IP address, a security protocol identifier and a security protocol identifier and a security parameter index, for example (see column 7, lines 25-37; column 3, lines 6-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Feiken et al** to use selectors to identify security association in the database because since a table contains one-to-many or many-to-many relationship of security information using an identifier would allow rapid retrieval of information since a secret key and other information may be associated with one identifier as suggested by **Leung**.

As per claims 68-69, the references as combined above disclose the limitation of wherein the one or more selectors include a destination IP address, a source IP address and a transport layer protocol and wherein one or more selectors further include a source port and a destination port (see **Leung**, column 7, lines 25-37 and column 9, line 52 through column 10, line 40) this is well-known in the art as included in IP header for performing IPsec processing and also disclosed in RFC 2401, "Security Architecture for IP" in Applicant's disclosure. Therefore, these claims are rejected on the same rationale as the rejection of claim 67 above.

As per claim 70, the references as combined above disclose updating or generating new security association in a database of the server to store security association information for the Home Agent that meets the recitation of wherein the step of determining security association information comprises if no security association information exists in the database associated with the packet, generating the security association information and storing the security association information in an entry in the database, for example (see **Leung**, column 7, line 50 through column 8, line 40). Therefore, this claim is rejected on the same rationale as the rejection of claim 67 above.

5. **Claim 63** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,484,257 to **Ellis** as applied to claims 46-62 and further in view of US Patent 6,708,273 to **Ober et al**.

As per claim 63, **Feiken et al** substantially discloses the claimed device of claim 46. **Feiken et al** does not explicitly disclose wherein the device is a network line card. **Ober et al** in an analogous art teaches a cryptographic co-processor implemented on a standard chip having encryption and hash circuits and other circuits (see column 2, lines 32-65 and column 5, lines 25-48 and abstract) within the same device for processing cryptographic operations in parallel (see column 6, lines 4-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the device of **Feiken et al** into a device such as a network line card because it would provide flexibility to incorporate the features of the device into any network device capable of using a network line card. The motivation to do so is also given by **Ober et al** who teaches that the plurality of encryption engines make it possible to add security to various processing applications. Hardware such as encryption and hash circuits are provided and structured to work together to provide accelerated encryption/decryption capabilities as suggested by **Ober et al** (see column 2, lines 32-65).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2436
October 20, 2008